

# Exhibit D

# The Value of Personal Data<sup>1</sup>

Marc van Lieshout

TNO, Van Mourik Broekmanweg 6, 2618 XE Delft, The Netherlands  
 Marc.vanlieshout@tno.nl

## Abstract.

This chapter discusses the value of personal data from two complementary perspectives: the value of personal data for firms and the value of personal data for individuals. The chapter starts with a short introduction into the rise of personal data markets – markets basically driven by the economic exploitation of personal data. Then the chapter discusses how firms assess the value of personal data. This can be done from different angles, such as stock value and revenues. Another inroad is the costs of data breaches. A second perspective which is discussed is the valuation of personal data by individuals. Some empirical studies are presented that show how individuals value their personal data and what choices they tend to make. The chapter concludes with placing these developments in the frame of the upcoming data protection regulation. Data protection by default has relevance when taking the empirical studies seriously.

**Keywords.** Behavioural economics; Data protection by design; Economic value of privacy; Personal Data Markets; Privacy

## 1 Introduction

Personal data are an important asset in today's data-driven society. A report by the Boston Consulting Group in 2012 stated that the value created through digital identities would amount to approximately 8% of GDP for the EU-27 countries [3]. With regard to personal data, a privacy paradox seems to exist: individuals state that they consider privacy to be important, but they hardly are willing to undertake action to protect their personal data. The sharing of personal information on social networking sites, and the provision of personal data in exchange for apps and other web-based services seem to support this view. However, several arguments can be presented to explain this apparent contradiction. For instance, users do not have a choice but to accept that they hand over their personal data in exchange for the service to be delivered. Or, the distinction which users make between what they consider privacy relevant and what not, is different from the formal distinction between 'ordinary' personal

---

<sup>1</sup> This chapter is largely a reproduction of Chapter 2 of the TNO-report: Roosendaal A. Lieshout, M van, Veenstra AF van (2014). Personal Data Markets. TNO report R11390. [10] The original chapter has been written by the author. It has been adapted for this publication. Please, quote the paper as: Lieshout, M van (2015). 'The value of personal data.' In: Camenisch, J.; Fischer-Hübner, S. et al. (Eds). Privacy and Identity 2014, IFIP AICT, vol. 457. Heidelberg, Berlin: Springer, pp. 26-38.

data and sensitive data. Another explanation is that although users seem to reveal quite some personal data when using social media, accepting a new app or buying something on the internet, they use informal strategies to protect their privacy (for instance by supplying incorrect personal information) [1, 9].

Literature in the field of behavioral economics shows that there is a very limited willingness to pay for the protection of privacy [1, 5]. People are willing to accept privacy intrusions when it serves their interests. One should therefore wonder whether privacy plays a role at all when personal data can offer financial benefits to individuals. Still, the fundamental right to privacy is not an issue that can simply be put aside.<sup>2</sup> One needs a more thorough analysis, both of how these personal data markets are organized and of how individuals appreciate the economic or monetary value of their data. In this chapter I will start with an introduction to the rise of personal data markets (section 2). The largest part of this chapter will be dedicated to the presentation and the discussion of the various ways in which the monetary value of personal data can be measured.

## 2 The market for personal data

Over the years, a number of studies have investigated the rise of personal data markets [3, 4, 14, 15]. The studies differ in their focus; two of them look at the overall impact of changes in the use of personal data [14, 15], one study is dedicated to the size and the features of the European markets on personal data [3] and a fourth study investigates the economic value of Individual-Level Consumer Data (ILCD) [4]. The WEF 2010 study highlighted the relevance of personal data as an economic asset that could be perceived as the new ‘oil’ [14]. The metaphor of personal data as oil is an interesting one. It covers both the use of personal data as a product in itself and as being a substance that is basic to a large number of economic activities. The WEF study was one of the first in capturing the phenomenon of ‘big data’ developments, and identified a number of interesting features of these developments. It introduced an - arguably contestable - distinction between types of personal data that enables a kind of classification of the data processing and collecting processes (based on either voluntary, observed or inferred data, see below). Due to the contested nature of the first category (data being provided ‘voluntarily’) the WEF changed its phrasing in follow-on reports in the more apt phrasing ‘personally provided’.<sup>3</sup>

The Boston Consulting Group presented a study in which it estimated the economic value of personal data markets in Europe, introducing a new inventory of relevant economic sectors [3]. The study arrives at an expected value of personal data markets of 8% of European GDP in 2020. It bases its forecast on a composite average of growth of some prominent economic sectors at present. The three most relevant ones are online communication and entertainment (Compound Average Growth Rate 22%), e-Commerce (CAGR 15%) and web-communities (100%). Given the present market size, a presumed CAGR of 22% over the next years would yield a market of €330 Billion in 2020 with consumer benefits of €670 Billion because of reduced pric-

---

<sup>3</sup> See the change in phrasing between [14] and [15] on this subject.

es, time savings (because of self-service transactions) and the valuation of free online services.

The US-based study on Data Driven Market Economies, published by the Data Driven Marketing Institute, on the role of Individual-Level Consumer Data (ILCD) in providing marketing services, estimated the size of the ILCD market to be about \$156 Billion, offering work to approximately 676,000 people in 2012. With a total US marketing and advertising market of \$298 Billion the contribution of ILCD-based marketing added up to slightly more than 50%. The largest contribution to the economic value of DDME is related to the direct (50%) and indirect (21%) exchange of ILCDs between firms, with only some 29% related to the collection of use of ILCD within a single firm [4] (p. 15-16). The role of personal data in marketing activities is manifold, and ranges from personalized targeting, to measuring benefits of marketing activities and lowering the entry costs for small firms (for which mass-advertising is too costly). The study indicates the relevance of DDME for stimulating technology development and realizing start-up entrepreneurship.

The relevance of personal data has a public element as well. Personal data are a prime asset for public services. Having access to (reliable) personal data may improve the efficiency of public services. The relevance of collecting, aggregating, analyzing and using personal data thus extends beyond monetary terms. An example is provided by Kaiser Permanente, a US-based health insurance firm, which has collected a database with over 3 million patient records. It offers patients fast access to their medical files, allowing them for instance to schedule an appointment and to receive text messages for prescription refills, leading to cost savings for Kaiser Permanente of many hundreds of thousands of dollars [7]. Meanwhile, the same data can be used to investigate correlations between incidences of diseases and use of medicines. By using data analytics, Kaiser Permanente discovered a correlation between use of anti-depressants by pregnant women and the incidence of a form of autism by newborns [14]. These results enable adapting medical practices in anti-depressant prescriptions for pregnant women.

Massive personal data collection can thus serve multiple purposes. The area identified in the US study relating to advertisement networks in online environments can be seen as a growing and interesting part of personal data markets. The market is expanding with the growth of personal data that people leave, knowingly or unknowingly, when using one of the several digital platforms they have at their disposal. An estimation presented in the BGC study mentions a growth figure of 45% per year through 2015 to a volume of 7 zettabytes, being the equivalent of more than 1,000 gigabytes of data for each person on earth [3]. The advertisement market has already matured to some respect, being based on a large number of 'Freemium' services; the business model of these Freemium services is quite simple: personal data in exchange for a free service. The personal data are, as indicated, the 'raw material' for added value services such as personalized and targeted advertisement.

A market of personal data brokers has emerged. Large service providers such as Google, AOL and Yahoo have taken over personal data brokers to secure their own position in this advertisement market. Google now owns a number of brokers such as AdMob and Double Click. Apple has its own ad-broker with iAd. The role of these ad-brokers is growing. The ad-broker MobClix for instance, matches 25 advertisement networks with 15,000 different apps that are looking for advertisers [14]. An

organization as BlueKai offers a data exchange platform that captures more than 30,000 attributes over 300 Million users. It handles over 75 Million auctions a day (an auction being a tool with which advertisement space is offered to potential advertisers; ad networks are the intermediaries between advertisers and those offering advertisement space) [14].

### **3 The value of personal data**

The digitization of communication and information has given rise to an abundance of data-sharing practices. People share details about their whereabouts, their moods and their activities through a multitude of platforms. They leave traces that go unnoticed for themselves, such as their geo-location when carrying a mobile phone, or their click behaviour. The value of this information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible, allowing them to learn about purchasing habits and strategies, and to make the best suited offers to their customers. As indicated above, it is not only the commercial value of personal data that is of interest. The public value of these data analytics can be substantial as well. An example is the provision of medical information by patients with rare diseases.<sup>4</sup> The network of patients with rare diseases started as a social interaction between these patients but resulted in an extremely interesting network with very interesting personal experiences in medical treatments and use of medicines for medical practitioners (and pharmaceutical agencies).

#### **3.1 The monetary value of personal data – a firm perspective**

To measure the monetary value of personal data, two main perspectives can be used. The first is by assessing the monetary value of the firm that collects, aggregates, processes, stores and/or disseminates the personal data. Various approaches are possible for this assessment [8]. The second perspective determines which monetary value persons attach to their data. This can be assessed in various manners as well and is covered in the next section.

To start with the monetary value of personal values from a firm's perspective, the OECD study mentioned before [8] distinguishes between three perspectives: one can look at the stock value of a firm, at the revenues of a firm or at the price of data records on the market. Alternatively, one can also look at the costs of a data breach and at the price of personal data on an illegal market. All of these approaches show some features of the value of personal data but all have specific drawbacks as well.

A general feature of data is that it can be sold over and over again without loss of its intrinsic value. The copy is just as good as the original, enabling multiple offers without loss of price or value. A single item of personal data thus will hardly have a commercial value. It is the composite of personal data that makes a commercial difference. Combining specific classes of personal data to profiles is another way to realise commercial value. Profiles can be created bottom up (using the available data to create meaningful subsets of data) or top down (using pre-configured profiles to

---

<sup>4</sup> See [www.patientslikeme.org](http://www.patientslikeme.org)

check in what group specific people would belong). Both forms of profiles add to the monetary attractiveness of personal data, since the grouping of data add to the original value of the data.

The stock value of a firm is a measure of trust in the firm's capacity to produce valuable revenues. It expresses the expectation of shareholders in the growth potential of the firm. For firms trading in personal data as their primary source of revenues, the stock value can be used as a proxy for the value shareholders attach to the data collected and the processes that turn the data into profitable products. However, stock values will fluctuate because of contextual factors that do not bear a direct relationship with the primary process of the firm. Fluctuations of stock prices can induce further fluctuations, as was shown by the introduction of Facebook to the stock market. Only in relatively stable markets one might expect a relatively stable relation between the value of a firm's shares and the revenues it realizes on the basis of its business activities.

The revenues of a firm may serve as a better proxy since it indicates real cash flows on the market, due to the firm's ability to sell products to customers. It enables cross-comparisons between firms acting on a similar market, since one would expect these firms to encounter similar problems in selling their products. The revenues per record may be an indication of the ability of a firm to overcome the complexity of the market, yielding higher revenues against lower costs. Revenues should be compared to the total number of data records a firm owns in order to yield a comparative indicator (revenues per data record in a specific period of time). A drawback of this method is that external factors may influence the prices third parties are willing to pay for specific data on the market, and that there may be a dependency on the total number of records a firm possesses (synergistic effects due to the fact that a firm is able to offer a larger sample of personal data records) [8].

Costs can vary considerably between firms and between markets. This may influence the value of personal data as well.

An example that shows the variance between the indicators above is provided by Experian [8]. Experian is a data broker. Over 2011, Experian reported total revenues of USD 4.2 Billion realized over 600 Million individual records and 60 Million business data records. Its stock value fluctuated between USD 10 and 12 Billion. Market capitalization thus is about USD 19 per record, and annual revenues were about USD 6 per record. Profits were roughly USD 1 per record. By means of comparison, I compared the situation of Experian with the situation of Facebook (see table 1). The stock market prices of Facebook have seen huge fluctuations since its introduction (from an initial USD 38 to a low USD 20 low per stock two months later to a value of USD 55 in December 2013).<sup>5</sup> Market capitalization of Facebook developed from USD 90 Billion at the start of its presence at the stock market up to USD 140 Billion in December 2013.<sup>6</sup> Over the past four quarters (Q4-2012 up to Q3-2013), Facebook earned a total of USD 6.9 Billion (with USD 2.0 Billion in 2013 Q3) and had a profit

---

<sup>5</sup> [http://en.wikipedia.org/wiki/Initial\\_public\\_offering\\_of\\_Facebook](http://en.wikipedia.org/wiki/Initial_public_offering_of_Facebook) (accessed March 17 2015)

<sup>6</sup> [http://en.wikipedia.org/wiki/Initial\\_public\\_offering\\_of\\_Facebook](http://en.wikipedia.org/wiki/Initial_public_offering_of_Facebook) (accessed March 6, 2015)

of USD 1.04 Billion (with USD 0.43 Billion in 2013 Q3).<sup>7</sup> Over this year (Q4 2012 – Q3 2013), Facebook has a market capitalization of USD 116 per subscriber, revenues of USD 5.75 per subscriber and a profit of USD 0.87 per subscriber. Though not all revenues are due to selling ads, a large part is. The market capitalization of Facebook thus is considerably larger than the market capitalization of Experian while other indicators are in the same range (though positive revenues and profits for Facebook only started at Q4 2012).

**Table 1.** Comparison between Experian and Facebook [8, 15]

	<b>Experian 660 M users</b>		<b>Facebook 1,1 B users</b>	
	Total value	Per record	Total value	Per record
Market Capitalisation	\$10-12 billion	\$19 (2011)	\$90-140 billion	\$110 (Q4-2012; Q3-2013)
Revenues	\$4 billion	\$6	\$6.9 billion	\$6.25
Profit	\$660 million	\$1	\$1.04 billion	\$0.92

The prices of personal data as these are sold at the market place offer another indicator. This price reflects the value purchasers attach to these data, which in turn will depend on the profitability purchasers expect to realize. The Financial Times offers an interactive sheet that enables calculating market prices for specific sorts of data.<sup>8</sup> It distinguishes between demographic data, family and health data, property, sport and leisure activities and consumer data. Demographic data such as age, gender, ethnicity, zip-code and education level are worth USD 0.005 per piece. Job information is worth USD 0.1 if being an entrepreneur up to USD 0.72 if being a health professional, pilot or non-profit worker. Over the five data categories, a total of 24 data entries can be discerned, each worth a specific (usually very modest) price. For information on credit history, criminal records, bankruptcies, convictions etc. of persons one has to pay USD 30-40 per record.<sup>9</sup> Firms specialize in inquiries for this kind of background information. Apparently, one is willing to pay higher prices for specific records of particular persons. Information that is available on black market prices shows that data on credit card numbers, personal health records and the like may cost in the range of 1

<sup>7</sup> <http://techcrunch.com/2013/10/30/facebook-q3-13-beats-with-2-02b-revenue-0-25-eps-with-49-of-ad-revenue-now-mobile/> (accessed March 6, 2015)

<sup>8</sup> <http://www.ft.com/intl/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html> (accessed March 6, 2015). BTW: in order to access these pages one has to register oneself, thus adding to the value FT derives from its subscribers!

<sup>9</sup> <https://ioptconsulting.com/ft-on-how-much-is-your-personal-data-worth/>, referring to <http://backgroundreport360.com/> (visited March 6, 2015).

– 30 USD per record, depending on the sensitivity of the data but also on the occurrence of data breaches (which provide new data on the market but may also lead to a saturated market) [15].

Data breaches themselves offer another inroad to measuring the value of personal data. A data breach as occurred to the Sony PlayStation Network between April 17 and April 19 2011 led to the theft of personal data of 77 Million subscribers. It led Sony to stop its services for 24 days. Together with the costs of recovering from the hack and the fines to be paid, the data breach cost Sony USD 171 Million, this being the directly attributable costs. Per subscriber this led to a cost figure of USD 2.20. The indirect costs (loss of subscribers, negative brand image which may lead to a decline of purchases of other equipment as well, impact on stock market prices) have been estimated at USD 1.25 Billion, being USD 16 per subscriber.<sup>10</sup> Stock market prices showed a dip of approximately 6% when Sony entered the stock market again, but it is hard to decide whether this is due to the data breach or to the overall fall of stock market prices that Sony experienced in the period February 2011 – November 2012 (steadily falling down from USD 37 to USD 9 over this period).<sup>11</sup>

Bringing the various perspectives together, we can conclude that calculating prices per data record helps in understanding the value of personal data. A calculation from general revenues or the stock value of a firm to a price per record offers some insight in the value that is represented by the personal records a firms owns. However, stock value is a measure that is very dependent on external influences that bear no relationship with the value of the personal data. Revenues and profit per data record seem to offer a better perspective on the value of these data records. From the illustration I presented it showed that, while Experian and Facebook are active on different markets, the value of the data records they own is more or less similar. Other methods to calculate the commercial value of personal data show that the direct commercial value of personal data is usually relatively low, except for sensitive data and very specific data. Data breaches represent a specific measure of the price of personal data as well. The Sony PlayStation data breach showed that the costs per subscriber of this breach surpassed the net profits that Facebook and Experian made in a year per subscriber.<sup>12</sup>

### 3.2 The monetary value of personal data – the individual perspective

I will now shift the perspective from the value firms attribute to personal data to the value individuals attribute to their personal data. This valuation could vary considerably between individuals. What one individual would consider to be highly private information (such as income or health data), another individual might not bother

<sup>10</sup> Juro Osawa, May 9 2011. ‘As Sony counts hacking costs, analysts see billion-dollar repair bill.’ *Wall Street Journal*.  
<http://online.wsj.com/news/articles/SB10001424052748703859304576307664174667924>  
(accessed March 6, 2015).

<sup>11</sup> <http://quotes.wsj.com/SNE/interactive-chart> (accessed March 6, 2015).

<sup>12</sup> Having only a few illustrations in which the price of personal data was calculated, the findings are only illustrative. More research is needed to turn the findings in more robust conclusions. However, this is outside the scope of this article.



to share or sell.<sup>13</sup> The case of Shawn Buckles is an interesting illustration of this last position.<sup>14</sup> Shawn Buckles, set up an auction in 2014 to sell his personal data to the highest bidder. The firm that offered the highest price for his personal data would acquire a subscription of a year to data that were collected on Shawn Buckles. These data encompassed his personal profile, his location track records, his train track records, his personal calendar, his email conversations, his online conversations, his consumer preferences, his browsing history, and his thoughts.<sup>15</sup> The highest bidder for this data set was The Next Web. This firm offered €350,- for the full data set. Shawn Buckles used the auction to raise awareness for the commercialization of personal data and the consequences for privacy.<sup>16</sup>

In dealing with how people value personal data I will present two perspectives. Firstly, people could attribute a specific monetary value to these data as exemplified by Shawn Buckles. This is the commercial value of personal data. It forms the counter part of the overview I presented in the preceding section. Secondly, one can investigate what people are willing to pay to keep personal data private. The reasons for keeping these data private could vary. Data could be seen as delicate or sensitive data which people want to keep for themselves. Besides that, people might not want to have data made public because they think the economic benefits do not outweigh the disadvantages (getting loads of advertisements for instance).

The role of personal data in today's society is undisputed. In a Eurobarometer Survey, stemming from 2011, 74% of respondents indicated that they accept that personal data need to be disclosed when participating in today's society [13]. The same number of people consider financial information, medical information and identity card numbers to be personal information. The survey showed that higher educated people and people living in West and North European countries are more sensitive to what they consider personal data [13].

In understanding what people value in privacy, the traditional economic models have been supplemented with models that look at behavioural features. These models study the impact of attitudes and preferences on choices people make. A number of mechanisms that influence behaviour have been identified [2, 6, 9, 12]. People perceive losses differently than gains, and are more willing to prevent a loss than achieving a similar gain (prospect theory) [2]. People tend to value situations nearby differently from situations further away (hyperbolic discounting [9]. People tend to value what they own higher than what they do not own (endowment effect) [12]. People are

---

<sup>13</sup> The webforum 'Patients like me' offers an example that shows that patients are willing to share sensitive and personal data, hoping it will help in improving treatments for the rare diseases which they suffer. See <http://www.patientslikeme.com/> (visited March 7, 2015).

<sup>14</sup> See <http://shawnbuckles.nl/dataforsale/> (visited March 7, 2015)

<sup>15</sup> <http://shawnbuckles.nl/dataforsale/>. While some of these data categories seem to be rather straightforward, some pose problems. Email conversations, for instance, do not only contain information on Shawn Buckles but could reveal information on those with whom he communicates as well. And what precisely Shawn Buckles considered to be his thoughts is not identified at his website.

<sup>16</sup> Shawn Buckles published a Privacy Pamphlet on his website. The Pamphlet intends to raise awareness for the way how personal data are used for marketing purposes, and how the market of personal data 'lures' people in the trap to sacrifice privacy for 'free' services.

risk averse and People tend to overvalue immediate rewards and undervalue long term rewards (instant gratification) [6]. People tend to mimic behaviour shown by predecessors: if many people already entered a specific site or social medium, it seem to be OK (informational cascading). [6] The absence of real choices may impact upon how people will behave. When one can only chose between accepting specific conditions and getting access to a service or rejecting the conditions and thus having no access to that service, one may be tempted to accept unfavourable or unclear conditions. This practice is well-known in the internet-economy. Many services are offered as a ‘take it or leave it’ option. For many youngsters it is absolutely prerequisite to have a subscription to Facebook, if one wants to keep in close contact with one’s friends, and thus one has to accept the conditions Facebook poses, whether one likes this or not.

Empirical research that tries to identify the relevant parameters of behaviour in order to understand how people assess the value of their personal data, is relatively scarce. An ENISA study mentions four papers dealing with an empirical field- or lab-related study of privacy behaviour [5]. ENISA itself performed a case study in which it investigated whether people are willing to pay for additional data protection [5]. When buying a ticket for the cinema, participants could choose between a number of – varying – offers. The minimum set of data asked was name, e-mail address and date of birth. Variations existed in the usage of the data (indicating that the e-mail address provided would be used for advertisement options) and a request for additional information (phone number). On top of this, in some experiments the price was kept the same for different options while in other options the price was different between the privacy-friendly and the privacy-unfriendly firm. The experiment was conducted as a lab experiment (with 443 participants), in which different options were offered in sequence, and as a hybrid field experiment (with more than 2,300 participants). The study showed that the privacy-unfriendly option was chosen by the majority of the participants when this ticket was 50 cent cheaper than the privacy-friendly offer. A minor part of 13% chose to pay the additional 50 cents. Without price difference, the majority of participants chose the privacy-friendly option. The experiment also showed that participants, when buying two tickets consecutively, remained to a large extent (142 of 152 participants) loyal to their first choice, even when they could swap from the more expensive to the cheaper ticket [5].<sup>17</sup>

In an experiment performed in 2011 Acquisti checked how people evaluated the willingness of people to pay for protection of their data vis-à-vis the willingness of people to accept the use of these data. The experiment was focused on revealing whether the gap between ‘Willingness-to-Pay’ and ‘Willingness-to-Accept’ as identified in several studies, exists as well when dealing with privacy and data protection issues.<sup>18</sup> The Willingness-to-Pay for the protection of personal data was relabeled as Willingness-to-Protect. This was juxtaposed against the Willingness-to-Accept: users were offered a financial reward in return for release of specific personal data. The

---

<sup>17</sup> This could identify those people who really care about their privacy. The study did not conclude on this matter since it could not be asked (being a purely observational study that was constructed such that no direct link to privacy was made in the design of the field study).

<sup>18</sup> This gap is identified in many studies. People tend to value what they own above what they do not own and are thus willing to pay a higher price for keeping what they have than for achieving the same when not having it. See [1, 2].

experiment was performed with 349 (female) participants in a shopping mall. The participants first filled in a quiz and then answered some sensitive questions, such as the number of sex partners the participants had had. After filling in the questionnaire, participants could either protect information (at a specific cost) or sell it. The bonus they received was a gift card which price was 10 USD if no sensitive information was provided and 12 USD when they were willing to provide the sensitive information. Different scenarios were tested. In one scenario first the cheaper gift card was presented and participants were then asked to provide more sensitive information in exchange for the more expensive gift card (Willingness to Accept). Another scenario started with participants having revealed sensitive information in exchange for the gift card of 12 USD and were then enabled to change to the cheaper gift card in exchange for protection of their sensitive data (Willingness to Protect). Other, more complex scenarios were added. The gift cards were real, and the participants were not informed that this was an experiment directed at testing the difference between WtP and WtA. The experiments validated the different attitudes with respect to WtP and WtA. When first offered the 10 USD card, 52% of the participants kept the card and decided not to go for the more valuable card at the expense of revealing additional information. The other way around, only 10% of the participants decided to exchange the 12 USD gift card for the 10 USD gift card in order to protect their data. When the two cards were offered consecutively, 42% chose the 10 USD card when this was offered first, while 27% chose the 10 USD card when this was offered second.

A final study worth mentioning is a study performed by Spiekermann in which she investigated the willingness of participants to pay for their own data which they had left on Facebook before [11]. The – hypothetical – situation Spiekermann sketched is the announcement by Mark Zuckerberg that he pulls the plug out of Facebook. Facebook participants could either buy their information back or have it destroyed. In a second scenario a third party took over Facebook. Participants had the choice to leave their data at the platform or to buy their data back. A third scenario offered participants a share in the revenues of the third party that took over Facebook. The experiment was performed with over 1,500 Facebook participants. The results of the experiment showed that the Willingness to Pay/Protect was lowest in the first option (money one was willing to pay in order to have data saved): €16,- (median). In the second option Willingness to Pay/Protect was higher: €54,- (median) for preventing the data were sold to a third party. In the option of sharing in the revenues, people assessed the value of their data considerably higher: €507,- (median). The study supported the existence of the endowment effect: when people feel they own their data (shown by the possibility to share in the revenues) they consider the value of their personal data higher than in the other two scenarios. Spiekermann concludes that psychology of ownership is more relevant than privacy concerns in explaining attitudes of people vis-à-vis their personal data.

## 4 Conclusions

The market for personal data is growing explosively. Expectations are of double digit growths in the coming years. New services will be developed on the basis of the collection, aggregation and dissemination of personal data. The value of new businesses

is hidden in the stock of personal data that can be collected. Personalised and targeted advertising enables offering services for free. Personal data are the new ‘oil’: they fuel new services and they can be used to deliver additional services, based for instance on profiles constructed of the aggregation of personal data. In estimating the value of personal data from a firm’s perspective, I used a number of proxies (such as stock market valuation, revenues or profits per data record). This yields some comparative indicators. They highlight different aspects of the valuation of personal data. Revenues and profits per data record are more reliable indicators than stock market value. Comparing the situation of Experian and Facebook, it showed that the revenues and profits per data record were almost similar. The impact of data breaches is high, as the Sony PlayStation data breach shows. Costs per subscriber were twice as high as the annual revenues per subscriber of Experian and Facebook.

Empirical studies on how people value their personal data and what they are willing to pay to protect personal data to be used are scarce. The few studies available indicate a sensitivity of individuals for ownership of data, and the relevance of concepts such as instant gratification (evaluating immediate returns higher than returns on the longer term), hyperbolic discounting (difficulty of evaluating costs at the longer term against benefits at the shorter terms), and endowment effects (the relevance of a sense of ownership). The privacy paradox (people indicate they care about privacy but do not act accordingly) is at least partly situated in these behavioural features. The direct valuation of personal data is shown to be modest in the case of Facebook. When some kind of ownership is introduced, people start to bother more about their data and want a fairer share of the revenues that can be realized with the data. The experiments done in this respect showed that people prefer a privacy friendly approach when it is for free but that they are hardly willing to pay for additional privacy protection. .

These mechanisms may help to understand how people deal with their privacy and may help to develop systems that meet these expectations. One issue that springs to mind is the interpretation of privacy by default (or, to be more precise: data protection by default) as this is mentioned in the General Data Protection Regulation (article 23). Behavioural economics shows that it is very relevant to have a high level of data protection as starting point (by default). People appreciate what they have. Any privacy feature already built in into a system will likely be appreciated as OK and ‘nice to have’. When this feature is offered as a choice it is likely that people will only accept it when it comes for free and does not impose any mental or financial effort. Designing data protection by default such that it makes initial decisions for individuals in protecting their privacy is one approach towards ‘nudging’ individuals into privacy protection, as Acquisti proclaims [1].

Another issue is whether the fundamental right to privacy can be traded away by making good offers for personal data. The right to privacy is a fundamental right and will always have to be balanced against other fundamental rights. The very moment privacy becomes a tradable good, other fundamental rights, such as non-discrimination, will be put under pressure. The emergence of personal data markets and the increasing importance of profiles encompass opportunities for various forms of discrimination, both on commercial markets (people who are excluded from specific services or people who are offered specific services at a higher price) and in the

public domain (health insurers who will use profiles to discriminate in health services and insurance packages offered).

A prominent issue that needs to be tackled in this discussion is the proximity of the right to data protection and the right to privacy. Both rights are safeguarded in the European Charter of Fundamental Rights. This is an interesting observation since the European directive on data protection (which is expected to be replaced by the General Data Protection Regulation within the coming two to three years) is based upon economic and not fundamental principles, namely the free flow of such data (as expressed in the full title of the directive). By uplifting the principle of data protection to the level of a fundamental right the European Parliament seems to lend more moral support to safeguarding this principle against market forces. In that sense, a preliminary conclusion can be – for the European situation – that sheer market forces are not sufficient to determine the price against which privacy and/or data protection can be traded away. This requires further study, especially with the advent of the era of big data and data analytics.

## 5 References

1. Acquisti, A.: Nudging privacy: The behavioural economics of personal information. *IEEE Security and Privacy*, 72-7 (2009)
2. Acquisti, A., Grossklags, J.: What can behavioral economics teach us about privacy?, in: Acquisti, A. S. Gritzalis, S. Di Vimercati, C. Lambrinoudakis (Eds.). *Digital Privacy: Theory, Technologies, and Practices*. Auerbach Publications, 363-379. ISBN: 1420052179 (2007)
3. BCG: The value of our digital identity. Boston Consulting Group (2012)
4. Deighton, J., Johnson, P. A.: The Value of Data: Consequences for insight, innovation and efficiency in the US economy. Harvard (2013)
5. ENISA: Study on monetizing privacy. An economic model for pricing online information. Brussels: ENISA (2012)
6. Hoogveld, N., Straathof, S.M.: De nieuwe privacyverordening en keuzemogelijkheden voor consumenten. *Privacy & Identity*, vol. 16, no. 6, 262-266 (2013)
7. Katibloo, F.: Personal Identity Management: Preparing for a World of Consumer – Managed Data. Forrester, 30 September (2011)
8. OECD: Exploring the Economics of Personal Data - A survey of methodologies for measuring monetary value. In: *OECD Digital Economy Papers* (2013)
9. Rabin, M.: Incorporating limited rationality into economics. *The Journal of Economic Literature*, 51, 528-43 (2013)
10. Roosendaal, A., van Lieshout, M. van Veenstra, Personal Data Markets. TNO report R11390, Delft (2014)
11. Spiekermann, S.: Privacy property and personal information markets. Acatech - Deutsche Akademie der Wissenschaften. Berlin (2012)
12. Thaler, R.: Towards a positive theory of consumer choice. *Journal of Economic Behavior and Organization*, 1, 39-60 (1980)
13. TNS-NIPO: Attitudes on Data Protection and Electronic Identity in the European Union. In: *Eurobarometer 359*. Brussels: European Commission (2011)
14. World Economic Forum. Personal Data: the emergence of a new asset class . World Economic Forum (2010)

15. World Economic Forum 2013. Unlocking the value of personal data: from collection to usage. World Economic Forum (2013)